5-2015

What's It Worth to Keep a Secret?

Gavin C. Reid

Nicola Searle

Saurabh Vishnubhakat
Texas A&M University School of Law, sv10@law.tamu.edu

WHAT'S IT WORTH TO KEEP A SECRET?

GAVIN C. REID, NICOLA SEARLE, SAURABH VISHNUBHAKAT[†]

ABSTRACT

This article is the first major study of protection and valuation of trade secrets under federal criminal law. Trade secrecy is more important than ever as an economic complement and substitute for other intellectual property protections, particularly patents. Accordingly, U.S. public policy correctly places a growing emphasis on characterizing the scope of trade secrets, creating incentives for their productive use, and imposing penalties for their theft. Yet amid this complex ecosystem of legal doctrine, economic policy, commercial strategy, and enforcement, there is little research or consensus on how to assign value to trade secrets. One reason for this gap is that intangible assets in general are notoriously difficult to value, and trade secrecy by its opaque nature is ill-suited to the market-signaling mechanisms that offer at least some traction in other forms of valuation. Another reason is that criminal trade secret law is relatively young, and the usual corrective approaches to valuation in civil trade secrecy are not synonymous with the greater distributive concerns of criminal law. To begin to fill this gap, we examine over a decade of trade secret protection and valuation under the U.S. Economic Espionage Act of 1996. From original data on EEA prosecutions, we show that trade secret valuations are lognormally distributed as predicted by Gibrat's Law, with valuations typically low on the order of $5 million but reaching as high as $250 million. There is no notable difference among estimates from various valuation methods, but a

---

[†] Dr. Gavin C. Reid is Dean of the Dundee Business School at Abertay University and Honorary Professor at St. Andrews University. Dr. Nicola Searle is an Economic Advisor at the United Kingdom Intellectual Property Office and Honorary Research Fellow at the University of St. Andrews. Saurabh Vishnubhakat is an Associate Professor of Law at the Texas A&M University School of Law and a Fellow at the Duke Law Center for Innovation Policy; until 2015, he was an Expert Advisor at the United States Patent and Trademark Office.
Sincere thanks to David Ulph, Felix Fitzroy, Arnab Bhattacharjee, Geethanjali Selvaretnam, Connie Luthy, Jeffery Dubin, Laurent Maderieux, and Nicole Finco for thoughtful feedback on successive iterations of this project, and to the Horowitz Foundation, the Russell Trust, and the University of St. Andrews Centre for Research into Industry, Enterprise, Finance and the Firm (CRIEFF) for financial support to Dr. Searle. The arguments in this writing are the authors' and should not be imputed to the UKIPO, to the USPTO, or to any other organization.

difference between high and low estimates on one hand and the sentencing estimates on the other. These findings suggest that the EEA has not been used to its full capacity, a conclusion buttressed by recent Congressional actions to strengthen the EEA.

TABLE OF CONTENTS

INTRODUCTION

Trade secrets are tremendously important . . . probably. Early in 2013, the Office of the U.S. Intellectual Property Enforcement Coordinator issued an administration-wide strategy to combat the theft of trade secrets.[1] The strategy echoed a commitment to protect American intellectual property aggressively, a goal which President Obama had set nearly three years earlier in a speech before the Export-Import Bank[2] and which presidents of both parties have increasingly articulated in recent times.[3] In mid-2012, the United States Patent and Trademark Office (USPTO) sent its first chief economist to testify before the House Homeland Security Subcommittee on Counterterrorism and Intelligence about the threat that economic espionage poses for U.S. economic security.[4] It was clear that the Subcommittee appreciated the complex interrelationship among intellectual property policy, economic analysis, border security, and law enforcement in protecting commercial secrets, for the slate of witnesses also included an assistant agency director for investigations from Immigration and Customs Enforcement and an assistant agency director from the FBI's counterintelligence division.[5] For its part, Congress, in the landmark Leahy-Smith America Invents Act of 2011, expanded the ability of prior

---

[1] WHITE HOUSE OFFICE OF THE IP ENFORCEMENT COORDINATOR, *Strategy on Mitigating the Theft of U.S. Trade Secrets* (Feb. 2013), *available at* www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[2] WHITE HOUSE OFFICE OF THE PRESS SECRETARY, *Remarks by the President at the Export-Import Bank's Annual Conference* (Mar. 11, 2010), *available at* www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference.

[3] *E.g.*, *Remarks by President George W. Bush at a Welcoming Ceremony for President Hu Jintao of China* (Apr. 20, 2006), *available at* www.gpo.gov/fdsys/pkg/WCPD-2006-04-24/html/WCPD-2006-04-24-Pg740.htm (calling for China, *inter alia*, "to improve enforcement of intellectual property rights"); *Remarks of President William J. Clinton at the World Trade Organization in Geneva Switzerland* (May 18, 1998), *available at* www.gpo.gov/fdsys/pkg/PPP-1998-book1/html/PPP-1998-book1-doc-pg807-2.htm (describing a joint U.S.-Japan commitment to "protect intellectual property" and, further, calling for broader consensus within the Asia-Pacific Economic Cooperation).

[4] House Homeland Security Subcommittee on Counterterrorism and Intelligence, *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security*, Hearing (June 28, 2012) (statement of USPTO Chief Economist Stuart J.H. Graham).

[5] House Homeland Security Subcommittee Counterterrorism and Intelligence, *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security*, Hearing, (June 28, 2012), *available at* www.homeland.house.gov/hearing/subcommittee-hearing-economic-espionage-foreign-intelligence-threat-american-jobs-and.

users of a secret product or process to defend against allegations of infringement under a later-issued patent on the given product or process.[6] In a separate provision of the same law, Congress also directed the USPTO to publish a report by January 2012 on how the protection of trade secrets through a prior user defense operates in the industrialized world.[7]

The reason the importance of trade secrets is in question, despite such strong institutional indicia, reflects the titular question of this article: far from being an academic or qualitative inquiry, the importance of trade secrets poses a quantitative challenge to estimate just how important, how valuable, how worth protecting they are. To help answer that question, this article offers a comprehensive study assessing the value of trade secrets based on original data from federal criminal prosecutions for trade secret misappropriation. Of particular interest are differences between the trade secret values estimated under various economic methods and the set of values actually employed in sentencing.

This article contains three parts. Part I summarizes the law and economics of trade secrecy and introduces the Economic Espionage Act of 1996. Part II presents an empirical study of criminal trade secret prosecutions, describing the econometric specification and data from the U.S. Department of Justice (DOJ), the Public Access to Court Electronic Records service, and other sources. Part III discusses the study's findings as well as their normative implications. First in this discussion is a descriptive view of U.S. federal criminal protection of trade secrecy, based on comparative estimates of trade secret value. Second is an assessment of key models for calculating damages and, accordingly, of how best to value trade secrets. Third is further statistical and econometric analysis of differences between high and low trade secret value estimates and cross-reference values. Fourth is a discussion of the criminal sentencing implications that follow from the multiplicity of possible trade secret valuations. The article concludes with an outlook for further research.

---

[6] Pub. L. No. 112–29 § 5 (Sept. 16, 2011), amending 35 U.S.C. § 273. The prior user defense had previously applied only to business methods and strategies. In 1998, the Court of Appeals for the Federal Circuit held in *State Street Bank & Trust Co. v. Signature Financial Group Inc.* that methods for doing business are patent-eligible subject matter under 35 U.S.C. § 101. *See* 149 F.3d 1368, 1375 (Fed. Cir. 1998). Congress responded the following year in the American Inventors Protection Act by creating a safe harbor for firms whose business methods and strategies could now be the subject of patents asserted against them. Pub. L. No. 106–113, § 4302 (Nov. 29, 1999).

[7] USPTO, REPORT ON THE PRIOR USER RIGHTS DEFENSE (Jan. 2012), *available at* www.uspto.gov/aia_implementation/20120113-pur_report.pdf.

I. THE CONTOURS OF TRADE SECRECY

Protecting trade secrets and penalizing their misappropriation has long been a part of commercial strategy.[8] It was in the nineteenth century, however, that Anglo-American common law formally recognized trade secrets as protectable interests.[9] Moreover, only in modern economic strategy have trade secrets emerged as a major mechanism for guarding the value of intangible assets.[10] Particularly in recent years, trade secrecy has risen in importance as a potentially attractive alternative in the face of dissatisfaction with aspects of the U.S. patent system,[11] including arguments that various characteristics of the current patent system can actively impede innovation.[12] As a result, a growing literature on appropriating value from knowledge assets now describes the value of trade secrecy relative to other mechanisms.[13] This literature has two dimensions: legal and economic.

A. The Legal Dimension

1. Trade Secrecy as Intellectual Property

As a legal matter, a trade secret is any information that is the subject of reasonable efforts to keep it secret and which derives independent economic value from the maintenance of its secrecy from others who can benefit economically from its disclosure—be it a "formula, pattern, compilation, program, device, method, technique, or process."[14] Having no formal registration requirement, trade secrecy originally arose state by state

---

[8] *See generally* Stephan R. Epstein, *Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe*, 58 J. ECON. HIST. 684 (1998).

[9] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As IP Rights*, 61 STAN. L. REV. 311, 315 (citing Vickery v. Welch, 36 Mass. (19 Pick.) 523 (1837), and Newbery v. James, (1817) 35 Eng. Rep. 1011 (Ch.)).

[10] *See, e.g.*, Josh Lerner, *The Importance of Trade Secrecy: Evidence from Civil Litigation*, Harv. Bus. Sch. Working Paper No. 95-043 (Dec. 1994).

[11] *See, e.g.*, ADAM B. JAFFE & JOSH LERNER, INNOVATION AND ITS DISCONTENTS: HOW OUR BROKEN PATENT SYSTEM IS ENDANGERING INNOVATION AND PROGRESS, AND WHAT TO DO ABOUT IT (2004).

[12] DAN L. BURK & MARK A. LEMLEY, THE PATENT CRISIS AND HOW THE COURTS CAN SOLVE IT (2009).

[13] *See generally* Wesley M. Cohen, Richard R. Nelson & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why US Manufacturing Firms Patent (Or Not)*, NBER Working Paper No. 7552 (Feb. 2000).

[14] Unif. Trade Secrets Act § 1(4) (providing a definition for "trade secret"). In a similar vein, the Restatement defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

as a common law right.[15] However, since the Uniform Trade Secrets Act was completed in 1979, that model code has been widely adopted in 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.[16] The modern trend toward interstate uniformity without outright federalization[17] has also produced a robust practitioner-oriented literature on a variety of subsidiary issues, such as regulatory compliance under the Sarbanes-Oxley Act[18] in accounting practices for trade secret assets,[19] trends in federal civil trade secret litigation,[20] criminal prosecution,[21] and criminal sentencing.[22]

For all its practical importance, however, trade secrecy has often been regarded as a doctrinal aberration in an intellectual property discourse that is occupied primarily by patents, trademarks, and copyrights.[23] Though these canonical forms of intellectual property are the subjects of their own

---

[15] Mary Witzel, *Protecting Pharmaceutical Trade Secrets Under the New Regulatory Sharing Program*, 41 AIPLA Q.J. 737, 742 (2013).

[16] NAT'L CONF. OF COMMISSIONERS ON UNIFORM STATE LAWS, "Uniform Law Commission Legislative Fact Sheet – Trade Secrets Act," *available at* www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act.

[17] The latest efforts to create a federal civil cause of action against misappropriation of a trade secret include the Future of American Innovation (FAIR) Act of 2013, S. 1770, 113th Cong. (1st Sess. 2013); The Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (1st Sess. 2013); and the Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2d Sess. 2012).

[18] Sarbanes–Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (July 30, 2002).

[19] *See, e.g.*, R. Mark Halligan, *Duty to Identify, Protect Trade Secrets Has Arisen: Sarbanes-Oxley Requires Internal Control Over How They Are Valued*, NAT'L LAW J., Aug. 29, 2005, at S3.

[20] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291 (2009).

[21] Mark L. Krotoski, *Common Issues and Challenges in Protecting Trade Secret and Economic Espionage Act Cases*, UNITED STATES ATTORNEYS' BULLETIN: ECONOMIC ESPIONAGE & TRADE SECRETS, Nov. 2009, at 2, *available at* www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[22] Christopher S. Merriam, *Addressing Sentencing Issues in Trade Secret and Economic Espionage Cases*, UNITED STATES ATTORNEYS' BULLETIN: ECONOMIC ESPIONAGE & TRADE SECRETS, Nov. 2009, at 62, *available at* www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[23] *See* R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, 6 No. 1 LANDSLIDE 12, 13 (2013) (noting that "[t]rade secrets have always been viewed as a stepchild intellectual property right"); Michael P. Simpson, *The Future of Innovation*, 70 BROOK. L. REV. 1121, 1122–25 (2005) (identifying and criticizing an historical progression of trade secret theory toward a grounding in intellectual property as distinguished from "traditional" subjects of intellectual property rights, including patents and copyrights).

debates as to purpose and form, they are all widely understood as sharing certain essential features. For example, all three are generally utilitarian incentive systems.[24] Moreover, all three draw their force from federal organic statutes[25] and elaborate regulatory regimes in order to provide a mechanism for excludably recouping investments in nonrival knowledge assets.[26] For the state-based law of trade secrecy, on the other hand, commentators have variously proposed doctrinal frameworks based in tort,[27] contract,[28] and traditional property[29]—while expressing doubt as to the conception of trade secrecy as intellectual property proper.[30] Nevertheless, there is now also a growing body of literature to support an intellectual property-based theory of trade secrecy.[31]

This literature is both normative and descriptive in its reach. For example, Professor Mark Lemley identifies the key components of such a framework with the incentives to invent and to disclose, and with protection

---

[24] *See, e.g.*, Rochelle C. Dreyfuss, "Patents and Human Rights: Where is the Paradox?" in INTELLECTUAL PROPERTY AND HUMAN RIGHTS: A PARADOX 74 (Willem Grosheide, ed.) (2010) (characterizing the traditional conception of intellectual property as a utilitarian mechanism for impeding free riders in order to foster innovation). *But see* Elizabeth L. Rosenblatt, *Intellectual Property's Negative Space: Beyond the Utilitarian*, 40 FLA. ST. U. L. REV. 441, 456–57 (2013) (defining and defending intellectual property under personality theory as a means for exercising "a fundamental right to oneself" inasmuch as the products of one's creative labor are "a manifestation of that self"); Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 330–65 (1988) (discussing more generally the personhood theory of intellectual property law).

[25] The federal patent laws are codified in Title 35 of the U.S. Code, the federal trademark laws in Title 15, and the federal copyright laws in Title 17.

[26] Economic theory has long recognized that knowledge has two important traits that make it difficult to create and easy to copy: first, it is non-rival, or capable of being used at the same time by infinitely many people without depriving any one of its use; second, it is not excludable, i.e., pragmatically difficult to deny to unintended parties. *See, e.g.*, Paul M. Romer, *Endogenous Technological Change*, 98 J. POL. ECON. S71, S74 (1990), *available at* pages.stern.nyu.edu/~promer/Endogenous.pdf.

[27] *See, e.g.*, C. Owen Paepke, *An Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, 2 HIGH TECH. L.J. 55 (1987).

[28] *See, e.g.*, Thornton Robison, *The Confidence Game: An Approach to the Law About Trade Secrets*, 25 ARIZ. L. REV. 347 (1983).

[29] *See, e.g.*, Miguel Deutch, *The Property Concept of Trade Secrets in Anglo-American Law: An Ongoing Debate*, 31 U. RICH. L. REV. 313 (1997).

[30] Edmund W. Kitch, *Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683 (1980).

[31] *See, e.g.*, Charles Tait Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. L. 39 (2007).

channels between patents and trade secrets.[32] Secrecy requirements in trade secret law provide what Lemley terms a gatekeeper function. Under this view, trade secrecy is not a pragmatic means of appropriating the value of inherently self-disclosing products, as those products have low or no excludability.[33] Thus, secrecy requirements raise the cost of secrecy to encourage disclosure of information that would otherwise remain secret while channeling to the patent system those self-disclosing inventions for which secrecy is futile.[34] Similarly drawing on intellectual property rationales but proposing a principled preference in favor of secrecy where circumstances warrant, Professor Jonas Anderson argues from patent reward theory that facilitating choice by the inventor of the proper protection regime—whether patent or trade secret—is the most efficient solution to the problem of free riding.[35]

2. Trade Secrecy and Employment

Closely related to these mechanisms of trade secret protection are the interactions through which parties exchange and potentially expose trade secret assets, particularly interactions between employers and employees. Early American trade secret law took it as virtually axiomatic that "when a party who has a secret in trade employs persons [subject to secrecy,] those persons cannot gain the knowledge of the secret and then set it up against their employer."[36] This protection of company knowledge through a duty of confidentiality has survived well into modern case law as well. For example, in *Metallurgical Industries v. Fourtek*, the Court of Appeals for the Fifth Circuit found in favor of an industrial zinc-recovery furnace manufacturer whose former employees had set up a competing firm using proprietary metal reclamation processes.[37] In fact, the court went further, imposing liability not only on the former employees but also on

---

[32] *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311 (2009).

[33] Professor Lemley's discussion draws on the distinction developed by Professor Katherine Strandburg between self-disclosing and non-self-disclosing inventions. *See* Katherine J. Strandburg, *What Does the Public Get? Experimental Use and the Patent Bargain*, 2004 WIS. L. REV. 81, 104–18.

[34] Lemley, *supra* note 32, at 313.

[35] *See* J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 962 (2011).

[36] Peabody v. Norfolk, 98 Mass. 452, 459 (1868) (citing Lord Cranworth's opinion in Morison v. Moat, 9 Hare 241 (1851), regarding the law on "breach of confidence").

[37] Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1197–98 (5th Cir. 1998).

their third-party client, who had benefited from the employees' breach of confidence.[38]

However, the protection of trade secrets against a breach of confidence has not been without limits, particularly where the owner itself has either compromised its secrecy or relinquished it altogether. For example, in *Group One v. Hallmark Cards*, the Court of Appeals for the Federal Circuit applying Missouri state law found that a proprietary method for producing decorative curled and shredded ribbon was no longer protectable as a trade secret once the owner had published it in a patent application, even though the alleged misappropriator was not aware of the publication.[39] The Federal Circuit affirmed a "property theory" view of trade secrecy that regards the status of the secret as the logical antecedent, rather than a "relationship theory" view that would have penalized misappropriation based on the expected connection of confidence between the owner of the secret and the alleged infringer, such as an employee.[40]

Moreover, the enthusiasm for protecting trade secrets has, in U.S. law, stopped short of a more general preference for covenants not to compete. As the Court of Appeals for the Sixth Circuit explained in the early years of the Sherman Antitrust Act, reasonably limited non-compete agreements are acceptable as an ancillary provision to generally pro-competitive ventures such as a sale of a business operation.[41] Judge Taft, in his limited endorsement of non-compete agreements, found reasonable only that "the seller should be able to restrain the buyer from doing him an injury which, but for the sale, the buyer would be unable to inflict. This was not reducing competition, but was only securing the seller against an increase of competition of his own creating."[42] This distinction has important practical ramifications for trade secrecy. For their part, non-disclosure agreements offer specific and limited protection for trade secrets.[43] By contrast, non-compete agreements directly curb the eventual economic harm that trade secret theft inflicts through greater competition using the misappropriated

---

[38] *Id.* at 1204 (explaining that "[t]he law imposes liability not only on those who wrongfully misappropriate trade secrets by breach of confidence but also, in certain situations, on others who might benefit from the breach").

[39] Group One, Ltd. v. Hallmark Cards, Inc., 254 F.3d 1041, 1051–52 (Fed. Cir. 2001).

[40] *See id.* at 1051.

[41] United States v. Addyston Pipe & Steel Co., 85 F. 271, 280–82 (6th Cir. 1898), aff'd, 175 U.S. 211, (1899). Judge (later Chief Justice) Taft's acceptance of reasonably limited covenants not to compete remains good law. *E.g.*, Business Elecs. Corp. v. Sharp Elecs. Corp., 485 U.S. 717, 737–38 (1988).

[42] *Addyston Pipe*, 85 F. at 280–81.

[43] *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (describing the extent of the property right in a trade secret as coextensive with the protective acts of the owner in guarding against the secret's disclosure to others).

information.[44] Yet, precisely because of their broader anticompetitive potential, these more potent non-compete agreements are generally suspect in U.S. law.[45] As a result, owners must protect their trade secrets through more piecemeal and, ultimately more costly, contractually tailored measures.

Meanwhile, examples abound of high-profile misappropriations, particularly in breaches of the employer-employee relationship. In the consulting sector, for example, restructuring advisory firm AlixPartners recently accused two of its former managing directors of stealing confidential information and trade secrets upon departing to work for McKinsey & Company.[46] AlixPartners also sought to enforce non-compete agreements against the departing directors.[47] In high technology, a seven-year case spanning much of the 2000s ended in the conviction of two

---

[44] *See* Guy Carpenter & Co., Inc. v. Provenzale, 334 F.3d 459, 466. The court explained:

> [I]f an employer gives an employee confidential and proprietary information or trade secrets in exchange for the employee's promise not to disclose them, and the parties enter into a covenant not to compete, the covenant is ancillary to an otherwise enforceable agreement because:
> (1) the consideration given by the employer [the trade secrets] in the otherwise enforceable agreement [exchange of trade secrets for promise not to disclose] must give rise to the employer's interest in restraining the employee from competing [employer has interest in restraining employee with knowledge of employer's trade secrets from competing] and
> (2) the covenant must be designed to enforce the employee's consideration or return promise [the promise not to disclose the trade secrets] in the otherwise enforceable agreement.

Id. (quoting Light v. Centel Cellular Co. of Texas, 883 S.W.2d 642, 647 n.14 (Tex. 1994) (emphasis added).

[45] *See* Princo Corp. v. Int'l Trade Com'n, 616 F.3d 1318, 1336 (noting that "agreements not to compete that might be suspect standing alone are regarded as reasonable when they are ancillary to a larger endeavor whose success they promote") (citing Polk Bros., Inc. v. Forest City Enters., Inc., 776 F.2d 185, 189 (7th Cir. 1985)) (internal quotations omitted). *See also* Ohio-Sealy Mattress Mfg. Co. v. Sealy, Inc., 585 F.2d 821, 831 (7th Cir. 1978) (describing a "horizontal agreement among potential competitors to develop a national brand and not to compete with each other in selling it [as] considerably more suspect than limitations imposed by a single independent manufacturer on its distributors as a condition of their distributorships").

[46] Ashby Jones, *AlixPartners Accuses Directors Heading to McKinsey of Trade-Secret Theft*, WALL ST. J., Apr. 10, 2014, *available at* blogs.wsj.com/law/2014/04/10/alixpartners-accuses-directors-heading-to-mckinsey-of-trade-secret-theft/.

[47] Complaint at 23–24, AlixPartners v. Thompson, No. 9523 (Ct. Ch. Del. Apr. 9, 2014), *available at* assets.law360news.com/0527000/527082/File-Stamped%20Complaint.pdf.

Silicon Valley engineers for stealing chip design documents from four former employers.[48] In heavy industry, during the late 2000s, metal component and assembly manufacturer Metaldyne successfully pursued departing employees, including a former vice-president and a metallurgist, for trying to sell powdered-metal manufacturing processes to rival companies.[49]

Prominent examples have also come from finance. In 2009, Goldman Sachs alleged that departing programmer Sergey Aleynikov had stolen computer code related to the firm's proprietary high-speed trading platform, and that Aleynikov planned to offer similar capabilities to his new employer, Teza Technologies.[50] While Aleynikov's conviction was pending on appeal, French multinational bank Société Générale was similarly vindicated in the criminal conviction of former trader Samarth Agrawal for stealing the bank's high-speed trading software, which he had planned to replicate for the Manhattan hedge fund Tower Research Capital.[51] The Court of Appeals for the Second Circuit later reversed Aleynikov's criminal conviction, holding that computer code could neither be a stolen "good" nor be "related to or included in a product that is produced for or placed in interstate or foreign commerce" for criminal purposes.[52] A separate decision in the United States District Court for the District of New Jersey went further, directing Goldman Sachs to pay Aleynikov's legal fees.[53] Nevertheless, Congress disagreed with these judicial conclusions about computer code as an economic good that is protectable under federal criminal law. Congress subsequently reaffirmed the importance of trade secrecy to intangible and informational assets such as software code and expanded the legal scope of trade secret protection to cover such assets via the Theft of Trade Secrets Clarification Act of 2012.[54]

---

[48] The former employers were NEC Electronics, Sun Microsystems, Transmeta, and Trident Microsystems. Natalie Weinstein, *2 Engineers Sentenced for Espionage*, CNET, Nov. 22, 2008, www.cnet.com/news/2-engineers-sentenced-for-espionage/.

[49] Megan Lampinen, *Former Metaldyne Employees Plead Guilty to Information Theft*, AUTOMOTIVE WORLD, Sept. 19, 2008, www.automotiveworld.com/analysis/70969-us-former-metaldyne-employees-plead-guilty-to-information-theft/.

[50] Ashby Jones, *Manhattan Jury Finds Former Goldman Programmer Guilty*, WALL ST. J., Dec. 10, 2010, *available at* blogs.wsj.com/law/2010/12/10/.

[51] Bon Van Voris, *SocGen Ex-Trader Agrawal Sentenced for Software Theft*, BLOOMBERG NEWS, Mar. 1, 2011, www.bloomberg.com/news/2011-02-28/ex-societe-generale-trader-gets-3-years-in-prison-for-theft-1-.html.

[52] United States v. Aleynikov, 676 F.3d 71, 73 (2d Cir. 2012).

[53] Aleynikov v. Goldman Sachs Grp., Inc., 2013 WL 5739137, No. 12–5994 (D.N.J. Oct. 22, 2013).

[54] Pub. L. No. 112–236 (Dec. 28, 2012).

The legislative debate specifically and unfavorably cited the Aleynikov reversal as the motivation for the new law.[55]

B. The Economic Dimension

Beyond legal doctrine, trade secrecy has likewise benefited in its economic dimensions from foundational analytical work by Professors Friedman and Landes and Judge Posner.[56] Further theoretical refinements to this work have addressed issues such as strategic delay, the dynamics of trade secret accumulation, the relationship of invention scale and the strength of property rights to the desirability of trade secrecy, the value of trade secret licensing relative to other forms of protection, the treatment of trade secrets in collaborative research and development relationships, and the impact of trade secrecy upon improvement in research and development performance.

Strategic delay, for example, may be modeled as a decision on the part of basic innovators not to patent their innovations—or, more precisely, not to develop their innovations for patentability—immediately.[57] An innovator firm often has an incentive to opt out of the patent system initially and proceed using trade secrecy in developing applications of its knowledge assets because of the relative immediacy with which rival firms may reverse engineer publicly introduced applications of the innovation or infer the innovation from the published patent application.[58] However, the nature of the incentive to delay rests on competing effects. A larger number of rival firms in the market tends to diffuse the innovation more quickly, which then influences the innovator firm to wait and appropriate more applications of its innovation and to share fewer remaining applications with rival firms.[59] At the same time, delay by the innovator firm also delays its own payoff with regard to already-developed applications.[60] The resulting maximization problem has a unique positive solution, meaning that the innovator firm will choose to delay introducing its applications by an optimal time and reap optimal discounted profits.[61]

Within the firm, optimal accumulation of trade secret assets may be a function both of investment in the protection of the firm's trade secrets

---

[55] 158 *Cong. Rec.* S6968 (daily ed. Nov. 27, 2012).
[56] *See generally* David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61 (1991).
[57] Carmen Matutes, Pierre Regibeau & Katherine E. Rockett, *Optimal Patent Design and the Diffusion of Innovation*, 27 RAND J. ECON. 60, 61 (1996).
[58] *Id.* at 63.
[59] *Id.* at 64–65.
[60] *Id.* at 64.
[61] *Id.*

and in employee compensation.[62] In practice, this is particularly important in hierarchically-modeled firms in which managers have access to all trade secrets at or below their managerial level. When such a firm wishes to protect trade secrets at a given managerial level, all higher-level managers will also have access to it, and the firm must compensate them all enough to keep them from defecting to rival firms.[63] As a result, such firms may find it more profitable to allow lower-level trade secrets to dissipate rather than pay to protect every last secret.[64] Thus, managers will tend to increase their own wage value by overinvesting in the protection of those trade secrets to which they themselves have access and by overcompensating their subordinates to prevent defection.[65] However, this overinvestment will come at the expense of higher direct cost to the firm in trade secret security as well as higher indirect cost to the firm in higher wages for superior managers, who face the same case with a wider array of the firm's trade secrets.[66]

As between an innovator firm and an imitator firm, the need and value of interfirm or public disclosure in order to exploit innovations are often at odds with the threat of imitation depending on the strength of available property rights in the innovation.[67] Modeling this relationship as duopoly competition where the innovator firm has various kinds of private, asymmetric information about the innovation reveals an inverse relationship between the strength of available property rights and the resulting tendency toward disclosure.[68] To wit, innovators tend to patent and fully disclose small innovations, to patent and only partially disclose larger innovations to manage imitation through licensing, and to rely primarily on secrecy for very large innovations.[69]

Broadening this comparison of intellectual property protections, when private returns from innovation are the same whether patenting or maintaining trade secrecy, social returns are greater where the innovator chooses secrecy with licensing over disclosure by patenting.[70] Because this effect results from the lack of an independent creation defense in patent

---

[62] Jan Zabojnik, *A Theory of Trade Secrets in Firms*, 43 INT'L ECON. REV. 831 (2002).
[63] *Id.* at 833.
[64] *Id.*
[65] *Id.* at 834.
[66] *Id.*
[67] James J. Anton & Dennis A. Yao, *Little Patents and Big Secrets: Managing Intellectual Property*, 35 RAND J. ECON. 1 (2004).
[68] *Id.* at 2–3.
[69] *Id.* at 3.
[70] Franco Cugno & Elisabetta Ottoz, *Trade Secrets vs. Broad Patents: The Role of Licensing*, 2 REV. L. & ECON. 209 (2006).

law,[71] secrecy is not superior to regimes of intellectual property protection such as copyright, where such a defense does exist.[72]

Summarizing this body of theoretical literature through a simple model illustrates a key objective of this article. Suppose that a trade secret with some determinable value L is at risk of theft with some probability p. The probability p itself depends on the vigilance of the firm that owns the trade secret in protecting its trade secrets. As the firm's expenditure x on preventing trade secret loss grows, its probability p of suffering misappropriation declines. Thus, $p = p(x)$ and decreases monotonically.[73] Aside from the risk of misappropriation, the firm may also lose its trade secret through accidental disclosure or reverse engineering with some probability q and so incurs some expenditure y to prevent this form of loss. Thus, $q = q(y)$ and also decreases monotonically. The firm's objective function is a minimand: to minimize the sum of (1) the expected loss due to trade secret dissipation, either by misappropriation or by accidental disclosure or reverse engineering, and (2) the cost of developing and implementing preventive procedures to protect trade secrets.

If the firm is selling one unit of output at a given cost, which is independent of the costs of protecting trade secrets, then the total expected loss EL, with x and y within the control of the firm, is expressible by the following function:

$$EL(x, y) = p(x)[1 - q(y)] + q(y)[1 - p(x)] + p(x)q(y)L + x + y$$

The first-order conditions for minimizing this function with respect to x and y may be re-expressed as:

$$L = -1 / [p'(1 - q)]$$

and

$$L = -1 / [q'(1 - p)]$$

Both must both be positive. Thus, the greater the value of trade secrecy and the more efficient the method of preventing trade secret loss, the greater the amount spent on protecting trade secrecy.

Indeed, this article is partly an empirical exploration of the Friedman-Landes-Posner theoretical framework and subsequent refinements: to put values to L and to determine the probability distribution and relative magnitudes of those values in accordance with the methods by which they are calculated. In doing so, this article also takes note of

---

[71] *Id.* at 212–13.

[72] *Id.* at 218–19.

[73] In simplified terms, a monotonic function is one that is everywhere increasing or everywhere decreasing, i.e., where $a \leq b$, $f(a) \leq f(b)$, and vice-versa.

increasing dissatisfaction over the last decade in both academia and industry with patenting as a means for protecting intellectual property,[74] and an increasing enthusiasm instead for using trade secrecy and related strategies, such as lead time advantage, be it to protect product innovations[75] or to raise profits and stimulate clustering without inhibiting technological spillovers.[76] For data with which to conduct the empirical exploration, federal criminal prosecutions pursuant to the Economic Espionage Act of 1996[77] (EEA) are a rich and largely untapped source of insight into trade secret valuation.

C. The Economic Espionage Act of 1996

The EEA was a legislative response to the perceived growing disparity between federal protections for disclosed inventions and creative works in the form of private civil causes of action in patent and copyright, as compared with the absence of federal protections for trade secrets.[78] Congress regarded the EEA to be all the more urgent because of the importance of "proprietary economic information" to the national security interests of the United States.[79]

As a matter of definition, the EEA distinguishes between trade secret misappropriation in the more conventional sense ("theft for pecuniary

---

[74] *E.g.*, ADAM B. JAFFE & JOSH LERNER, INNOVATION AND ITS DISCONTENTS: HOW OUR BROKEN PATENT SYSTEM IS ENDANGERING INNOVATION AND PROGRESS, AND WHAT TO DO ABOUT IT (2004).

[75] *E.g.*, Wesley M. Cohen, Richard R. Nelson & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why US Manufacturing Firms Patent (Or Not)*, NBER Working Paper No. 7552 (Feb. 2000).

[76] *E.g.*, Sudipto Bhattaccharya & Sergei Guriev, *Patents and Trade Secrets: Knowledge Licensing and Spillovers*, 4 J. EUR. ECON. ASS'N 1112 (2006). Professors Bhattaccharya and Guriev contrast knowledge licensing and spill-overs under patenting and trade secrets in a model which treats trade secrets as so-called "closed" sales of intellectual property. A closed sale aims to preclude the disclosing of trade secrets to the research departments of rival firms. The greater the value of interim knowledge and the greater the leaking of this knowledge, the more attractive the closed sale will be. *See also* Andrea Fosfuri & Thomas Rønde, *High Tech Clusters, Technology Spillovers, and Trade Secret Laws*, 22 INT'L J. INDUSTRIAL ORG. 45 (2004) (arguing that trade secret protection based on punitive damages increases trade secret spillover and clustering).

[77] Pub. L. No. 104–294, 110 Stat. 3488 (1996) (codified as amended in sections of 18 and 42 U.S.C.).

[78] *See* H.R. REP. NO. 104–788, 104th Cong., 2d sess. 4–7 (1996) (discussing the growing importance of proprietary economic information and explaining the need for legislation).

[79] *Id.*

gain")[80] and economic espionage ("theft for the benefit of a foreign entity").[81] Important to both, however, are three procedural safeguards. First is the availability of protective orders to safeguard the integrity of trade secrets during otherwise public prosecutions of their theft.[82] Second is specific authority for the EEA to have extraterritorial reach,[83] in contrast to the general principle that acts of Congress have force only within the territorial jurisdiction of the United States.[84] Third is limited prosecutorial discretion in pursuing possible violations of the EEA. Originally, this safeguard was quite limiting, as approval was initially necessary from senior officials in the DOJ with respect to both economic espionage and trade secret theft. This requirement is now somewhat relaxed, and DOJ prosecutors have greater independence with respect to pursuing trade secret theft cases.[85]

Beyond these important but ultimately straightforward parameters, the empirical valuation of the stolen trade secrets has since become central to enforcement of the EEA. Valuation is the foremost inquiry, whether in selecting cases to prosecute,[86] determining the length of sentence to impose, or establishing the magnitude of fine to assess.[87] Yet neither the text nor the legislative history of the EEA directly discuss the complex issue of trade secret valuation, and during the EEA's initial enforcement in the late 1990s, it was expected that the federal criminal justice system would look for valuation guidance in case law applying the Uniform Trade Secrets Act.[88]

---

[80] Charles Doyle, *Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832*, Congressional Research Service Report No. R42681, July 25, 2014, at 1–9, *available at* www.fas.org/sgp/crs/secrecy/R42681.pdf.

[81] *Id.* at 9–11.

[82] *Id.* at 11. *See generally* 18 U.S.C. § 1835; United States v. Hsu, 155 F.3d 189, 193–94 (3d Cir. 1998) (protecting trade secrets unless they are essential to defend against the case).

[83] Doyle, *supra* note 80, at 11–12.

[84] *Id. See generally* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010); Charles Doyle, *Extraterritorial Application of American Criminal Law*, Congressional Research Service Report No. 94–166, Feb. 15, 2012, *available at* www.fas.org/sgp/crs/misc/94-166.pdf.

[85] Doyle, *supra* note 80, at 12 (citing U.S. DEPARTMENT OF JUSTICE, CRIMINAL RESOURCE MANUAL § 1122).

[86] *See* FED. BUREAU OF INVESTIGATION, REPORTING THEFT CHECKLIST, *available at* www.justice.gov/criminal/cybercrime/reportingchecklist-ts.pdf. (noting that the FBI asks victims to place the estimated value of the stolen trade secret within a range.)

[87] Marc J. Zwillinger & Christian S. Genetski, *Calculating Loss Under the Economic Espionage Act of 1996*, 9 GEO. MASON L. REV. 323 (2000).

[88] *See, e.g., id.* at 328–337 (comparing lost profits, disgorgement, reasonable royalty, and replacement cost approaches for determining loss in civil trade secret

Indeed, the House Judiciary Committee report on the EEA only briefly discussed that "the very conditions that make this proprietary information so much more valuable make it easier to steal,"[89] and that, "[g]iven the increased use of electronic information systems, information can now be stolen without asportation and the original usually remains intact."[90] Yet, this well-theorized nonrival and variously nonexcludable nature of information[91]—enabling, e.g., theft without asportation—drives not only value and theft risk in trade secrets, but also difficulty in valuation.

Like the employer-employee cases discussed above,[92] a recent case illustrates the large values at risk from trade secrecy theft, the gravity with which federal enforcement institutions treat such theft, and the variability of valuation even when culpability is clear and the economic loss thoroughly documented. In June 2010, biotechnology research scientist Kexue Huang was indicted for misappropriating and transporting trade secrets to the People's Republic of China while working for Dow AgroSciences LLC.[93] A separate indictment in 2011 additionally charged Mr. Huang with stealing a trade secret from Cargill Inc.[94] On October 18, 2011, Dr. Huang pled guilty both to economic espionage against Dow AgroSciences and to trade secret theft against Cargill, admitting the estimated aggregate loss from his criminal conduct to be in the range of $7 million to AgroSciences and $20

---

cases and noting the relevance of these approaches to criminal prosecutors, defense attorneys, and judges alike in evaluating loss under the EEA).

[89] H.R. REP. NO. 104–788, *supra* note 78, at 4–5.

[90] *Id.* at 11.

[91] *See, e.g.*, Henry E. Smith, *Intellectual Property As Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742 (2007); R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 1001–16 (2003). By contrast to this understanding, however, Professor Christopher Yoo has suggested that copyright is excludable and partially nonrivalrous, making it an imperfect public good at best. *See* Christopher S. Yoo, *Copyright and Public Good Economics: A Misunderstood Relation*, 155 U. PA. L. REV. 635 (2007); Christopher S. Yoo, *Copyright and Product Differentiation*, 79 N.Y.U. L. REV. 212 (2004).

[92] *See supra* notes 46–54 and accompanying text.

[93] U.S. DEPARTMENT OF JUSTICE OFFICE OF PUBLIC AFFAIRS, *Chinese National Charged with Economic Espionage Involving Theft of Trade Secrets from Leading Agricultural Company Based in Indianapolis* (Aug. 31, 2010), *available at* www.fbi.gov/indianapolis/press-releases/2010/ip083110a.htm. *See* United States v. Huang, No. 1:10-CR-00102 (N.D. Ind., filed June 16, 2010).

[94] Karen Gullo, *Ex-Dow Scientist Who Stole Secrets Gets 7 Years, 3 Months Prison*, BUSINESSWEEK, Dec. 22, 2011, www.businessweek.com/news/2011-12-22/ex-dow-scientist-who-stole-secrets-gets-7-years-3-months-prison.html. *See* United States v. Huang, No. 1:11-CR-00163 (N.D. Ind., transferred in Sept. 9, 2011) (giving the history of the case against Huang).

million to Cargill, respectively.[95] The court ultimately sentenced Mr. Huang to seven and a quarter years in prison.[96] Importantly, the Huang prosecutions also reflect a more basic distributive problem in attempting to describe the more publicly protected value of trade secrets in the criminal context, in contrast with the corrective private remedy appropriate to the civil context.[97]

Thus, although civil trade secret valuations still remain the polestar of guidance in valuation for criminal cases,[98] it is of no small consequence that trade secret protection under the EEA has also benefited in recent years from broader debate about the proper scope of trade secrecy at the federal level.[99] Moreover, greater study of intangible asset valuation in patents,[100] copyrights,[101] and trademarks[102] has produced a literature ready for similar study on trade secrets.

---

[95] *See* DEPARTMENT OF JUSTICE, *supra* note 93.

[96] Gullo, *supra* note 94.

[97] Jason M. Solomon, *What Is Distributive Justice*, 44 LOY. L.A. L. REV. 317, 323 (2010) (observing that the concern of civil justice with rectifying imbalances makes it "distinct from retributive or distributive justice"). Professor Solomon identifies three principal dimensions of difference between civil and criminal justice notwithstanding that both attempt to redress moral injuries: (1) the different exercises of agency by the individual or the state in prosecuting civil versus criminal wrongs; (2) the individual's interest in private vindication and empowerment versus the state's interest in retribution and deterrence; and (3) the nature and degree of disapprobation awaiting the wrongdoer in a civil remedy, such as money, versus in a criminal remedy, such as imprisonment. *Id.* at 327–28.

[98] *See* Zwillinger & Genetski, *supra* note 87.

[99] For example, former Senator Herbert Kohl in October, 2011, introduced an amendment of 18 U.S.C. § 1836 to create a federal civil private cause of action under the EEA over and above the existing authority of the Attorney General to seek injunctive relief. *See* S. Amdt. 729, 112th Cong. (1st Sess. 2011).

[100] *See, e.g.*, Malcolm T. Meeks & Charles A. Eldering, *Patent Valuation: Aren't We Forgetting Something? Making the Case for Claims Analysis in Patent Valuation by Proposing a Patent Valuation Method and a Patent-Specific Discount Rate Using the CAPM*, 9 NW. J. TECH. & INTELL. PROP. 194 (2010); Michael S. Kramer, *Valuation and Assessment of Patents and Patent Portfolios through Analytical Techniques*, 6 J. MARSHALL REV. INTELL. PROP. L. 463 (2007); F. Russell Denton & Paul J. Heald, *Random Walks, Non-Cooperative Games, and the Complex Mathematics of Patent Pricing*, 55 RUTGERS L. REV. 1175, 1181–93 (2003).

[101] *See, e.g.*, Matthew J. Baker & Brendan M. Cunningham, *Court Decisions and Equity Markets: Estimating the Value of Copyright Protection*, 49 J.L. & ECON. 567 (2006); John M. Gabala, Jr., *"Intellectual Alchemy": Securitization of Intellectual Property As an Innovative Form of Alternative Financing*, 3 J. MARSHALL REV. INTELL. PROP. L. 307 (2004).

II. PROSECUTIONS UNDER THE EEA

To that literature, this article makes three principal contributions. First, using an original dataset, we analyze the size distribution of the values of the EEA trade secrets. Second, we examine evidence of statistical differences between estimates of trade secret values, using different valuation methods and arriving at surprising results about the commonality of intent in courts' valuation methods. Finally, we find statistically significant differences both between high and low estimates of trade secret value and between valuations argued during prosecution and those employed at sentencing.

A. Data and Descriptive Statistics

This study examines 95 EEA prosecutions involving 147 defendants during the period of 1996–2008. Data is from statements and releases that the DOJ has issued about prosecutions the Criminal Division has conducted, especially the Computer Crime and Intellectual Property Section of that division,[103] and from the Public Access to Court Electronic Records (PACER) service.[104] Once identified, EEA cases prosecuted under 18 U.S.C. § 1832 were further analyzed using docket reports, *viz.*, lists and summaries of judicial proceedings such as appearances and actions; underlying court documents regarding filing and termination dates, sentences, fines, and conviction; and journalistic accounts discussing qualitative details such as the victim's relationship to the defendant, the alleged value of the stole trade secrets, and parallel civil actions. Not least, academic publications also yielded information about particular cases in the context of the EEA.[105] The quantitative and qualitative evidence gathered from this wide range of data sources enables a robust inferential discussion beyond the descriptive accounts published to date, and supports greater normative discussion of the use and theft of trade secrets and of relevant available policy levers.

---

[102] *See, e.g.*, Espen Robak, *Lessons from Nestle v. Comm'r: Second Circuit Rejects Popular Trademark Valuation Method*, 26 J. CORP. TAX'N 135 (1999); GORDON V. SMITH, TRADEMARK VALUATION (1997).

[103] UNITED STATES DEPARTMENT OF JUSTICE, *available at* www.justice.gov/.

[104] PUBLIC ACCESS TO COURT ELECTRONIC RECORDS, *available at* www.pacer.gov/.

[105] These include Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Applications of the Economic Espionage Act and the TRIPS Agreement*, 78 N.Y.U. L. REV. 1475 (2003); Chris Carr & Larry R. Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25 (2001); Chris Carr, Jack Morton & Jerry Furniss, *The Economic Espionage Act: Bear Trap or Mousetrap?*, 8 TEX. INTELL. PROP. L.J. 159 (2000); Zwillinger & Genetski, *supra* note 87.

B. Econometric Model

The threshold econometric question of how trade secrets are likely distributed in their value looks to the observed values of stolen trade secrets that have come to light in EEA prosecutions. The expected distribution is lognormal,[106] owing to a combination of Gibrat's Law of Proportional Effects[107] and the Central Limit Theorem.[108] The reason for this expectation is that, as applied to firms, Gibrat's Law posits that the growth rates of firms are a random process and are independent of their initial size, e.g., as measured by assets. That is, because firm size is distributed lognormally, the underlying growth process is proportionate.

More formally, if size is measured by assets, then given an asset value A_t at time period t, the change in asset size over one time period is a random proportion of its size in the previous period:

(1) $A_t - A_{t-1} = \varepsilon_t A_{t-1}$

where ε_t has mean zero and is serially uncorrelated. From this, it follows that the growth rate of A_t is expressible as:

(2) $(A_t - A_{t-1}) / A_{t-1} = \Delta A / A_{t-1} = \varepsilon_t$

Taking the summation of both sides of equation (2) over a number of periods I shows that:

(3) $\sum_{(t=1 \text{ to } \tau)} (\Delta A / A_{t-1}) = \sum_{(t=1 \text{ to } \tau)} (\varepsilon_t)$

Moreover, if one lets the finite change in assets ΔA in the numerator of the left hand side of equation (3) tend toward the small differential dA, and therefore going to the integral from the sum, then in the limit, the following approximation holds:

(4) $\sum_{(t=1 \text{ to } \tau)} (\Delta A / A_{t-1}) = \int_{(\text{from } A_0 \text{ to } A_\tau)} (dA / A) = \ln A_\tau - \ln A_0$

which is equal to the right hand side:

(5) $\sum_{(t} \varepsilon_t)$

---

[106] *See generally* Brian E. Smith & Francis J. Merceret, *The Lognormal Distribution*, 31 C. MATHEMATICS J. 259 (2000), *available at* www.jstor.org/stable/pdfplus/10.2307/2687413.pdf (explaining that lognormal distribution is a probability distribution in which the logarithm of the random variable takes a normal distribution).

[107] *See* Jan Eeckhout, *Gibrat's Law for Cities*, 94 AMER. ECON. REV. 1429 (2004); ROBERT GIBRAT, LES INÉGALITES ÉCONOMIQUES (1931).

[108] *See generally* David A. Thomas, *Understanding the Central Limit Theorem*, 77 MATHEMATICS TEACHER 542 (1984), *available at* www.jstor.org/stable/pdfplus/10.2307/27964198.pdf (explaining that the theorem predicts that, for a set of independent random variables, each with a well-defined expected value and variance, the mean of such variables will be approximately normally distributed).

Given initial asset value A_0, equations (3), (4), and (5) are expressible as:

(6) $\ln A_I = \ln A_0 + \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_I$

By the Central Limit Theorem, the right-hand side of equation (6) will, in the limit as $I \rightarrow \infty$, be normally distributed. Thus, the distribution at equilibrium of the logarithm of asset value $\ln A$ may be denoted as:

(7) $\ln A \sim N(\mu, \sigma^2)$

which is a normal distribution having mean μ and variance σ^2. By definition, if the natural logarithm of A is normally distributed, then A is lognormally distributed, denoted as:

(8) $A \sim \ln(\mu, \sigma^2)$

Thus, Gibrat's Law of Proportional Effects results in a lognormal equilibrium distribution of assets.

Moreover, applied to trade secrets, Gibrat's Law implies that, for a firm whose trade secrets have an asset value of A in a given year, each trade secret asset generates, or can have imputed to it, an annual income Y for the firm. If the annual rate of interest is r, then the following simple proportional relationship will hold:

(9) $Y = r \times A$

This proportion reflects a premise that industry practice confirms: the designated value of a trade secret is often based on the income stream attributable to that trade secret.

C. Valuation Models

A review of trade secret valuation models reveals important considerations for their application. Three major sets of models merit discussion: income models, cost models, and market models.

1. Income Models

The income models—unjust enrichment, lost profits, and reasonable royalty—base the valuation of the trade secret on cash flow analysis. These models have theoretically robust foundations, and the discounted cash flow approach in particular is a standard tool in financial analysis.[109] This standardization suggests that, not only are firms more likely to be familiar with income models of valuation and related methods, but also that they constitute a well-theorized and therefore potentially powerful legal tool for litigants and courts.

---

[109] *See generally* JAMES R. HITCHNER, FINANCIAL VALUATION: APPLICATIONS AND MODELS (2d ed., 2006).

The Uniform Trade Secrets Act itself supports the use of income models. The model act states:

> Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.[110]

The UTSA's reference to "actual loss" suggests that valuation of the trade secret may properly include lost profits, actual damages, or both. The use of the income models in UTSA cases also underscores the high analytical regard in which these models are held and implicitly connects the considerable case law surrounding the UTSA with broader questions of trade secret valuation.

Particularly among the income models, the reasonable royalty model is appealing as it can be implemented regardless of the actions of the alleged misappropriator or thief. Unlike the unjust enrichment and lost profits models, which both require actual unauthorized use of the trade secret, the reasonable royalty model is universally applicable.[111]

Despite this high regard, useful grounding in the case law, and wide applicability, the EEA data show only one identified case involving the use of reasonable royalty. Indeed, income models more generally were used in only one-third of all EEA cases studied. Thus, in spite of its theoretical potential from an economic perspective, the method is not popular in practice. Reasons for this relative disuse may range from pragmatic concerns about the relative economic incentives and payoffs associated with the reasonable royalty model (or income models more generally),[112] to more foundational cultural differences between more theoretically oriented economic arguments and more pragmatically inclined legal institutional

---

[110] UNIFORM LAW COMMISSION, UNIFORM TRADE SECRETS ACT § 3, *available at* www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[111] *See* Zwillinger & Genetski, *supra* note 87, at 342–46 (arguing for the use of the reasonable royalty model in EEA cases as being most in line with Sentencing Guidelines). To wit, Zwillinger and Genetski argue that: "When ascertainable, this [reasonable royalty] measure values stolen information at the moment and in the context of the misappropriation, and it takes into account, but does not exclusively rely upon, the defendant's intention to exploit information."

[112] *Cf.*, *e.g.*, Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991 (2007) (advancing both theoretical and empirical arguments in the patent context that the reasonable royalty model tends, at least in component industries, systematically to overcompensate patent owners for inventions that are part of larger products rather than compensate them in proportion to the incremental value of the patented invention).

actors[113]—particularly as reasonable royalty calculations, unlike other models, rely entirely on a hypothetical agreement between a willing licensee and willing licensor, an exercise fraught with its own analytical challenges.[114]

2. Cost Models

The cost models—research and development, replacement costs, and actual damages—are based on the idea that the trade secret is worth the amount that it cost its owner to develop or protect, or would cost to redevelop. These models, too, are involved in approximately one-third of the EEA cases identified here for study. Significantly, innovative firms are likely to keep good accounts of research and development costs, a tendency that makes the model appealing for its ease of application.[115] In practice, however, research and development investment alone may not represent the empirical minimum value, as comparison of the cost models in EEA cases shows.[116]

With regard to usage of the cost models, the actual damages approach was involved in five cases, representing 17% of the EEA cases with identified trade secret value estimates. Despite the lack of theoretical robustness—e.g., damages associated with the misappropriation could, to varying degrees, be independent of the underlying value of the trade secret—calculation of actual damages presents a fairly straightforward legal matter. The victim must merely present evidence of the direct costs resulting from the theft.

---

[113] *See, e.g.*, JULES L. COLEMAN, THE PRACTICE OF PRINCIPLE: IN DEFENCE OF A PRAGMATIST APPROACH TO LEGAL THEORY 13–24 (2001) (criticizing prevalent approaches to the economic analysis of tort law for inadequately representing the full complexity of that body of legal doctrine).

[114] *Cf., e.g.*, Elyse Dorsey & Matthew R. McGuire, *How the Google Consent Order Alters the Process and Outcomes of Frand Bargaining*, 20 GEO. MASON L. REV. 979, 983 (2013) (noting the importance of *ex ante* versus *ex post* perspectives on investing in a patented technology rather than a next-best alternative and the associated problems of switching costs, lock-in, and—in the undesirable case—holdup by the patentee). The problem can be even more challenging in the reputationally charged realm of enjoining copyright infringement. *See* Jiarui Liu, *Copyright Injunctions After Ebay: An Empirical Study*, 16 LEWIS & CLARK L. REV. 215, 264 (discussing doctrinal concerns peculiar to copyright).

[115] *See* MARK A. GLICK, LARA A. REYMANN & RICHARD HOFFMAN, INTELLECTUAL PROPERTY DAMAGES: GUIDELINES AND ANALYSIS 337 (2002) (arguing that "the owner's investment in the trade secret can be used as a proxy for the trade secret's minimum value").

[116] *See infra* Part 0 (discussing the lack of statistically significant difference among the average values generated by using cost models in the EEA cases identified for study).

3. Market Models

Market models seek to define a fair market value of the trade secret. The Sentencing Guidelines favor the use of fair market value, when available:

> The fair market value of the property unlawfully taken or destroyed or, if the fair market value is impractical to determine or inadequately measures the harm, the cost to the victim of replacing that property.[117]

However, the market models have generated the widest range of trade secret valuations of the three types of models. This variation is likely due to the relative subjectivity in measuring fair market value as compared to other models. The reported range actually represents a conservative estimate, as the removed outlier—$108 million in the Lucent case[118]—was calculated using fair market value approach. The use of fair market value estimates is limited by the type of trade secret: that is to say, there may be a limited market for the trade secrets in question as they are often quite industry- or technology-specific. Bid information, for example, has no legitimate fair market value, as no legal market exists for bid information. As a result, while the sentencing guidelines may call for the utilization of fair market value, its application is neither straightforward nor widespread.

III. DISCUSSION

From this framework, the estimated values of stolen trade secrets in EEA prosecutions are variously grouped by the valuation model used for estimation, as well as by low, high, and cross-reference estimates. The low, or conservative, estimates receive greater emphasis in accordance with prior literature.[119] Low and high estimates are deflation-adjusted to 2008 values.

A. Estimates Across Valuation Models

Analysis of the EEA data initially reveals apparent differences among trade secret value estimates produced by different valuation methods. Table 1 presents cases according to the valuation method used, based on low estimates. In cases where an estimate of the stolen trade secret was published, roughly two-thirds identified the estimation method that the court used. As mentioned above, one observation was removed as a

---

[117] U.S. DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES 332 (4th ed. 2013), *available at* www.justice.gov/criminal/cybercrime/.

[118] *See infra* note 119 and accompanying text.

[119] *See, e.g.*, Carr & Gorman, *supra* note 105.

clear outlier—an estimate of $108 million for the Lucent source code derived using the market value method.[120]

Similarly, comparing valuation methodologies against the resulting value estimates, using the low estimates, shows marked clustering of values at the lower end of the scale. This is consistent with previous findings of lognormality in the distribution of estimated trade secret values, where the cases proportionally most prevalent are associated with very low value estimates.

However, the distribution of these values across calculation methods does not, at least for the small sample of 21 observations, indicate systematic differences among value estimates produced by these valuation methods.[121] This lack of observed differences in the observed means of the various models admits of two explanations.

One explanation is that, while different valuation models do produce meaningfully different value estimates, the sample size of 21 observations is too small to detect such differences. However, the estimates generated here have relied on small sample distribution theory to mitigate this problem, suggesting an alternate explanation. That is, no meaningful difference exists among the methodological premises of the various valuation models. The diverse valuation methods are based on the same economic theory, and merely approach the goal from different directions. What is more, although different valuation methods may, in practice, produce somewhat different valuations for the same trade secret, no systematic difference need result across the methods themselves.

Nevertheless, though trade secret value estimates may not vary significantly from one valuation model to another, comparison across high, low, and cross-reference estimates reveals a quite different story, one with

---

[120] United States v. ComTriad et al, No. 2:01-cr-00365 (D.N.J., filed May 31, 2001) (noting that, in the Lucent case, the source code technology that the defendants stole was generating on the order of $100 million in sales for Lucent in 2000. This was deemed an outlier because it is five times the value of its closest neighbor and seven standard deviations from the mean).

[121] Two tests confirm the absence of statistically significant differences among the various valuation methods. First is the analysis of variance (ANOVA) test, which here yields the following diagnostics: $F = 1.11$, and prob value = 0.39, indicating lack of significance in the differences. Second is the student's t-test for differences between the means of various categories of valuation—i.e., grouping methodologies as income models, cost models, and market models—which here yields prob value = 0.80 for cost vs. income, prob value = 0.50 for cost vs. market, and prob value = 0.28 for cost vs. market, all indicating a lack of significance in the differences. Notably, all of these tests were conducted using logarithmically transformed observations to take account of the known lognormality of the variables.

important normative implications for the protection of trade secrets under federal criminal law. As a point of departure for these comparisons, it is helpful first to understand how trade secret values are statistically distributed.

B. Distribution and Comparison of Trade Secret Values

As shown in Figure 1, the majority (79 percent) of stolen trade secrets are worth less than $5 million. The sample size for low value estimates is 29 observations; the mean of low estimates is $4.47 million, the standard deviation is $9.95 million, and the mode—i.e., the value for a maximum on the probability density—is much lower. The distribution of Figure 1 strongly suggests lognormality and is defined only for positive values of the variate, is unimodal, and is strongly positively skewed, with a typical long tail stretching to positive infinity. Lognormality at a larger sample would predict a smoother long right tail for the probability density. A formal test of lognormality appears in Figure 2, where all data points are within the 95 percent confidence interval and the corresponding linear function is fitted by maximum likelihood.[122]

Similar results hold for the high estimates, as shown in Figure 3, where the mean value is $26.3 million, the standard deviation is $88.7 million, and the modal value is again well below the mean. Moreover, as shown in Figure 4, the high estimates all lie within the 95% confidence interval[123] and thus reflect a lognormal distribution for the same reasons as the low estimates discussed in Figures 1 and 2.

C. Differences in Estimation

1. Low and High Estimates

---

[122] Further confirmation comes from the Anderson-Darling (AD) test for departures from normality. *See generally* Michael A. Stephens, *Tests Based on EDF Statistics*, *in* RALPH B. D'AGOSTINO & MICHAEL A. STEPHENS, GOODNESS-OF-FIT TECHNIQUES (1986). In general, the greater the AD statistic, the less the support for a hypothesis of lognormality. Conversely, the larger the probability value, the less the ability of the test to reject a null hypothesis of lognormality. The AD statistic in Figure 2 enables comparison between distributions where smaller values are preferred. Here, the AD statistic for the lognormal distribution (AD = 0.6) is lowest as compared to several alternate distributions. The probability value calculation, based on the AD statistic, gives p-value = 0.108. As the null hypothesis is that the data reflect a lognormal distribution, and the p-value in this case is greater than 0.05, the null hypothesis is not rejected with 95 percent confidence, and the distribution of low estimates in trade secret value is, indeed, lognormal.

[123] The Anderson-Darling statistic (AD = 0.48) is even lower, with p-value = 0.221.

Because most trade secrets in the analysis have two estimated values—a low estimate and a high estimate—it is possible to test for a statistical difference between them using a paired t-test. As shown in Table 2, the sample size is restricted to those cases in which the high estimate is distinct from the low estimate. Though this reduces the sample size to 16 observations, the results agree with those of the unreduced sample. Based on the previously determined lognormality of the sample, the test is run on the natural logarithms of the estimated values.

Although the high and low estimates are correlated,[124] the paired t-test indicates that the means of the two samples are statistically different.[125] Economically, this difference is highly meaningful in that it reflects as much as a $39.6 million difference between high and low estimates, based on the untransformed values of the means. A further non-parametric test, the Wilcoxon test, confirms on weaker assumptions that the statistical difference between the two samples is highly significant.[126] Moreover, just as Figures 2 and 4 give strong evidence of lognormality in the distribution of trade secret value estimates, the probability plot of the relation between high and low estimates shown in Figure 5 both reaffirms the lognormality of value estimates generally and highlights the differences between the high and low estimates.

The implications of this statistical difference between high and low estimates are far-reaching. The alleged value of the stolen trade secrets affect—sometimes strongly—everything from the reporting of trade secret theft,[127] to the decision to prosecute,[128] to sentencing determinations. Substantial differences in estimated value for the same trade secret increases uncertainty for owners of trade secrets and support the problematic view that valuation is sensitive to the viewpoint, and interests, of the party offering the value estimate. Given the high burden of proof in criminal prosecution, this presents a problem for achieving justice when sentencing trade secret misappropriators and thieves.

---

[124] The coefficient of correlation is 0.46, significant at 10 percent.

[125] The mean of ln(high) is 2.58 more than the mean of ln(low), significant at 1 percent.

[126] The Wilcoxon test gives p-value = 0.00.

[127] Victims are required to estimate the value of the trade secret when reporting the theft. *See* U.S. DEP'T OF JUSTICE, *Reporting Intellectual Property Crime: A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets*, *available at* www.usdoj.gov/criminal/cybercrime/AppC-ReportingGuide.pdf.

[128] *Cf.* Paul Shukovsky et al, *The Terrorism Trade-Off*, SEATTLE POST-INTELLIGENCER, Apr. 11, 2007, at A1, *available at* 2007 WLNR 6959916 (discussing post-9/11 FBI fraud-enforcement as a policy of "triage" in which losses below $150,000 were unlikely to be investigated at all, and losses as high as $500,000 were "much less likely" than before September 11, 2001, to be investigated).

2. Cross-Reference Values

Resolving this problem requires going beyond simple comparison of high and low estimates to estimate trade secret values in EEA cases. The additional step is to apply a cross-referencing method that uses a combination of actual sentences and sentencing guidelines.[129] Such guidelines associate the offense level with a corresponding loss figure. Starting with a base offense level of 6 points to reflect the DOJ recommendation,[130] the figure is adjusted up by two levels for convictions that include economic espionage or crimes committed by defendants considered to be insiders of the company.[131] Based on incarceration periods adduced from PACER docket reports and on the offense level, the corresponding magnitude X_{ref} of trade secret loss may be estimated using the 2008 Sentencing Guidelines as follows.

First, the incarceration period of the convicted defendant is cross-referenced with the number of offense points given by the sentencing guidelines, as shown in the first column of Table 3. Because the incarceration ranges overlap, using the midpoint of each range best approximates the defendant's incarceration period. Second, as Table 4 shows, the offense level is calculated using information about the defendant from case documents and reports. Third, the value derived from Table 4 is subtracted from that derived in Table 5. The remainder is cross-referenced with the stolen trade secret values dictated by the Sentencing Guidelines, and the corresponding value, in the second column of Table 5, is X_{ref}.[132]

This method produces loss estimates for 41 cases. The X_{ref} values for these cases had a mean of $241,300 with a standard deviation of $579,700. As shown in Figure 6, the mean value of X_{ref} is much lower than is the mean for either the high or low estimates of trade secret value that was previously discussed. The mode is much lower than that of the high or low estimates. Moreover, though Figure 6 suggests a lognormal distribution, statistical analysis fails to confirm this conclusion.[133]

---

[129] *See* Zwillinger & Genetski, *supra* note 87, at 324 (arguing generally that "the United States Sentencing Guidelines' (Guidelines) reliance on fair market value as the linchpin of criminal culpability can be incomplete in certain EEA cases, and a holistic sentencing approach allowing for the consideration of additional factors would provide a more just result").

[130] *See* U.S. DEP'T OF JUSTICE, *supra* note 117, at § IV.F (discussing penalties for the theft of commercial trade secrets prosecuted under 18 U.S.C. §§ 1831–1839).

[131] *See* Zwillinger & Genetski, *supra* note 87, at 326–28 (discussing the application to EEA cases of sentencing guidelines).

[132] This method is, of course, the reverse of how courts actually sentence, first calculating offense points and then deriving the incarceration period.

[133] A comparison of four different probability distributions—Weibull, lognormal, normal, and log-logistic—appears *prima facie* to favor a log-logistic distribution

That the X_{ref} values do not follow the same distribution as the high and low values suggests that the X_{ref} values fundamentally differ from the other two valuations. Indeed, as Tables 6 and 7 show, the trade secret loss estimates used in sentencing (X_{ref}) are lower, to a statistically significant degree, than both high and low estimates. Moreover, as the distribution of X_{ref} does not take a lognormal distribution, neither does $\ln(X_{ref})$ take a normal distribution. Accordingly, a paired t-test is inapt to test for differences between X_{ref} and other valuations.

Better suited is the non-parametric Wilcoxon signed-rank test, which does not require normality in the underlying distributions. The Wilcoxon signed-rank test compares the difference between the values of each pair, sorts all nonzero absolute differences into ascending order to assign ranks, and calculates the test statistic from the sum of the ranks for positive and negative differences.[134]

Tables 6 and 7 compare high and low estimates, respectively, to the cross-reference estimate X_{ref}. The mean of X_{ref} values is significantly lower than that of high estimate values[135] and lower even than that of low estimate values.[136]

These differences further indicate that courts are using considerably lower cross-reference values than even the low estimates generated by various valuation models. The difference in raw means between cross-reference and low estimates is as much as $6.45 million. Accordingly, the values used in sentencing are lower, to a statistically significant degree, than those argued in the course of the court case. Put another way, the basis for punishment is lower than the basis for the crime as prosecuted.

---

over the lognormal distribution: the lognormal distribution has an AD statistic of 2.04, whereas the log-logistic has an AD statistic of 2.10. However, the test statistics for these distributions results in a rejection of the null hypotheses (of lognormal or log-logistic distribution) with a p-value of 0.01 in both cases. Therefore, the data do not conform to any of these classical probability distributions.

[134] The test statistic is as follows:

$$Z = [\ \min(S_p, S_n) - (n(n+1)/4)\ ] / \sqrt{[\ n(n+1)(2n+1)/24 - \sum(j=1 \text{ to } l)\ (t_j^3 - t_j)/48)},$$

where

n = number of cases with non-zero differences;

l = number of ties;

t_j = number of ties;

S_p = sum of positive ranks; and

S_n = sum of negative ranks

[135] The Wilcoxon test statistic $Z = -3.44$, and prob value = 0.001.

[136] The Wilcoxon test statistic $Z = -2.80$, and prob value = 0.005.

D. Implications of Valuation Differences

The statistically significant difference between high and low estimates and their own disconnection from the cross-reference values that courts use—all for the same trade secret—is cause for concern with respect to the impact of the economic policy animating criminal trade secret protection in the United States.

In particular, because the analysis in an EEA case of the magnitude of loss resulting from trade secret misappropriation largely determines sentencing—including whether the defendant will be imprisoned—even slight variations in the estimated loss can be quite meaningful.[137] The evidence discussed here demonstrates that empirically observed sentences of incarceration may be lower because courts have chosen to apply trade secret valuations that are particularly conservative.

This may reflect systematically successful arguments by defendants for the application of the lower values, particularly given the postures of prosecutor and defendant on opposing ends of the bargaining relationship and the statistically lower values used in sentencing guidelines. It may also reflect judicial modesty in appreciation of the difficulties facing the valuation of trade secrets and a consequent conservatism in favoring lower value estimates. Indeed, an examination of three case studies revealed that "the department essentially went in the tank on two of them and just said, 'We cannot value [the trade secret],' and [defendants] got probation."[138]

Moreover, in addition to the complexity of valuation methods, the goal of the values used in sentencing (i.e., X_{ref} values) is not solely that of determining a fair market value:

> The purpose of the Guidelines is to achieve sentences that accurately reflect the culpability of offenders in a consistent, uniform and proportional manner. In attempting to adhere to both the letter and purpose of the Guidelines, sentencing courts often struggle to make a fair market value determination. . . . In EEA cases, where the actual or intended loss to the victim or gain to the defendant can be disproportionate to the market value of the trade secrets, use of the

---

[137] Zwillinger & Genetski, *supra* note 87, at 341.

[138] UNITED STATES SENTENCING COMMISSION, Symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offenses, Session on Economic Espionage, at 276 (Oct. 13, 2000) (transcript of discussion by David Green, Joseph F. Savage, Jr. & Carla Mulhern), *available at* www.ussc.gov/Research_and_Statistics/Research_Projects/Economic_Crimes/20001012_Symposium/uGroupThreeDayTwo.PDF.

> market value determination alone will not always produce a sentence that is just.[139]

Indeed, the discrepancy between the values argued in the course of the case and those used in sentencing reflects a recognition by the court that these values may overestimate the actual or intended loss or gain. Thus, the criminal context of the EEA may play a large role in accounting for the statistically significant differences between these values.

Nonetheless, while the evidence indicates a favorable environment for would-be trade secret misappropriators and thieves, it lowers the incentives to innovate. Given the wide variability of the valuation methods and the evident use of lower value estimates in practice, the trade secret owner faces increased uncertainty as to the strength of the protection provided by trade secrets.

CONCLUSION

In sum, trade secret misappropriation and theft currently face diminished disincentives, and trade secret owners confront the uncertainty of diverse value estimates and, indeed, diverse methodologies of valuation. This uncertainty, particularly as it drives enforcement, therefore reduces the practical worth of trade secrets to owners, as a weakly protected trade secret has lower expected value to its owner. While infringement and damages payments may be beneficial for the patent owner, such benefit presupposes a patent-protected research tool.[140] Because trade secrets by definition derive value from their secrecy, the weaker the protection of this value, the lower the appropriable rewards to innovation.[141] Thus, greater uncertainty associated with the protection of trade secrets lowers incentives to innovate where trade secrecy is a meaningful mechanism for appropriating value from innovation.

The EEA sought to increase the overall protection for trade secrets, to unify the legal status at the federal level, and to provide protection against foreign economic espionage. Notwithstanding concerns articulated in the legal literature that the EEA may go too far in increasing the strength and definition of trade secrets,[142] empirical evidence regarding calculations

---

[139] Zwillinger & Genetski, *supra* note 87, at 353.

[140] *See, e.g.*, Mark Schankerman & Suzanne Scotchmer, *Damages and Injunctions in Protecting Intellectual Property*, 32 RAND J. ECON. 199 (2001).

[141] *Cf.* Alan C. Marco & Saurabh Vishnubhakat, *Certain Patents*, 16 YALE J.L. & TECH. 103 (discussing the economic importance in patent law of reliable mechanisms for rights enforcement to the practical value of the patent right, and empirically characterizing this relationship by estimating cumulative abnormal returns in stock market reactions to patent litigation decisions in the federal courts).

[142] *See, e.g.*, Carr et al, *supra* note 105.

of damages in EEA cases suggests that the EEA is not being used to its full capacity. Indeed, this evidence is consistent with affirmative steps that even the generally contentious 112th Congress took to strengthen the use of federal criminal trade secret protections, first by broadening the jurisdictional element of the EEA through the Theft of Trade Secrets Clarification Act of 2012,[143] and again by increasing the maximum fines permitted under the EEA through the Foreign and Economic Espionage Penalty Enhancement Act of 2012.[144]

To the intellectual property rights literature of industrial organization, this article contributes a publicly developed database that is well suited to examining the values of trade secrets from the perspective of diverse calculation methods. Parametric comparisons reveal that estimates of trade secret value do not vary significantly across valuation methods for the same trade secret. High and low estimates of trade secret value are lognormally distributed, as predicted by Gibrat's Law, and are statistically significantly different. By contrast, cross-reference estimates of trade secret valuations are distributed neither lognormally nor according to any classical probability density, and differ statistically from high and low estimates alike.

More generally, we conclude that the value that trade secrets create reflects an important economic role for trade secrecy in the larger sphere of intellectual property protection. The current body of trade secret literature, both theoretical and empirical, proceeds largely by reference to a more robust and faster-growing body of patent literature. A review of the methods used to assess damages in trade secret cases under the EEA confirms that the methods themselves rely heavily on analytical and empirical development in patent cases. However, their application to trade secret cases is complicated by the secret nature and legal ambiguity of trade secrecy as compared with the disclosure-oriented body of patent law.

As to further study, data on EEA prosecutions provides a unique opportunity for continuing empirical analysis of the use of trade secrets, their value, and the nature and consequences of their misappropriation. The possibility of biases in the selection of cases for prosecution represents a potentially valuable thread of research. Also potentially fruitful is an extension of the patent damages models used in trade secret valuation analysis, particularly if such an extension contributes to the development of new valuation models specific to trade secrets while taking account of the doctrinal and enforcement concerns that are peculiar to trade secrecy.

---

[143] *See supra* note 54 and accompanying text.
[144] Pub. L. No. 112–269 (Jan. 14, 2013).

TABLES AND FIGURES

Table 1: The Estimated Value of Trade Secrets by Valuation Method

Low Estimates of Trade Secret Value Using Various Methods EEA Cases 1996–2008				
	Method	**Mean**	**Std. Dev.**	**No. of Cases**
(i)	Unjust Enrichment	$ 5,728,000	$ 6,422,000	4
(ii)	Lost Profits	$ 708,000	$ 411,000	2
(iii)	Reasonable Royalty	$ 1,000,000	—	1
(iv)	R&D	$ 10,968,000	$ 18,950,000	4
(v)	Actual Damages	$ 207,000	$ 390,000	5
(vi)	Market Value	$ 10,145,000	$ 13,832,000	5 (1 outlier removed)

Figure 1. Probability Density of Trade Secret Value, Low Estimates

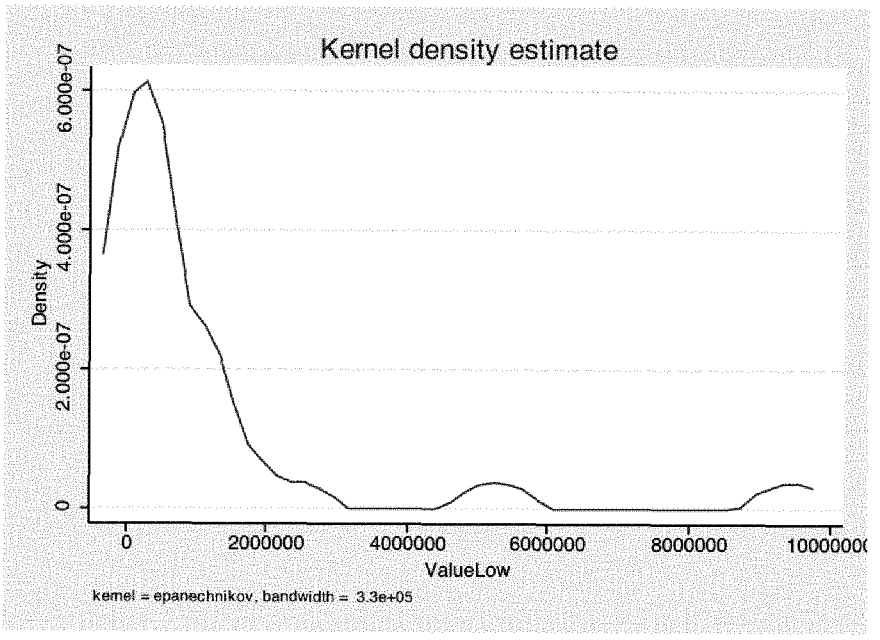

Figure 2. Confidence Intervals, Lognormally Distributed Low Estimates

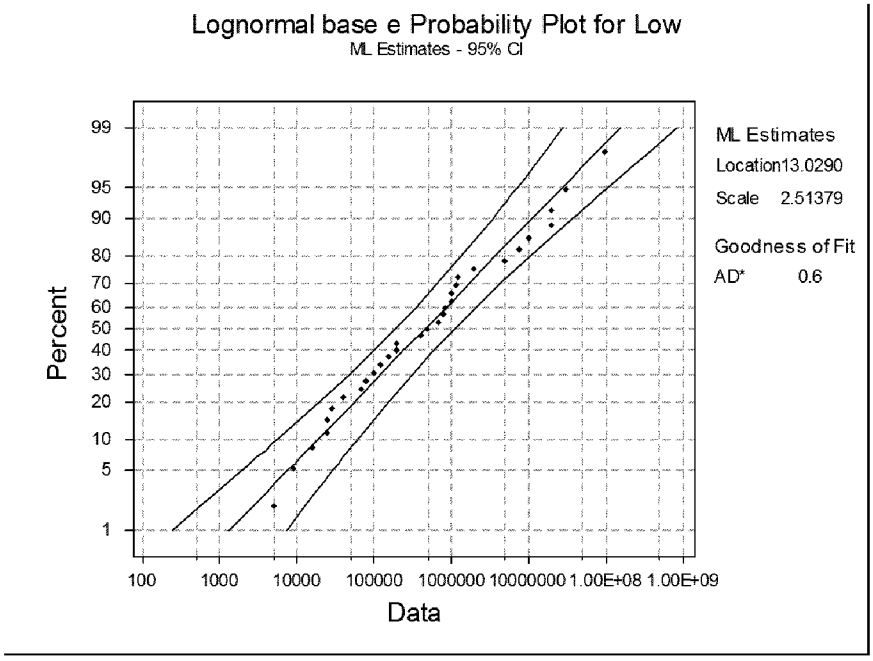

Figure 3. Probability Density of Trade Secret Value, High Estimates

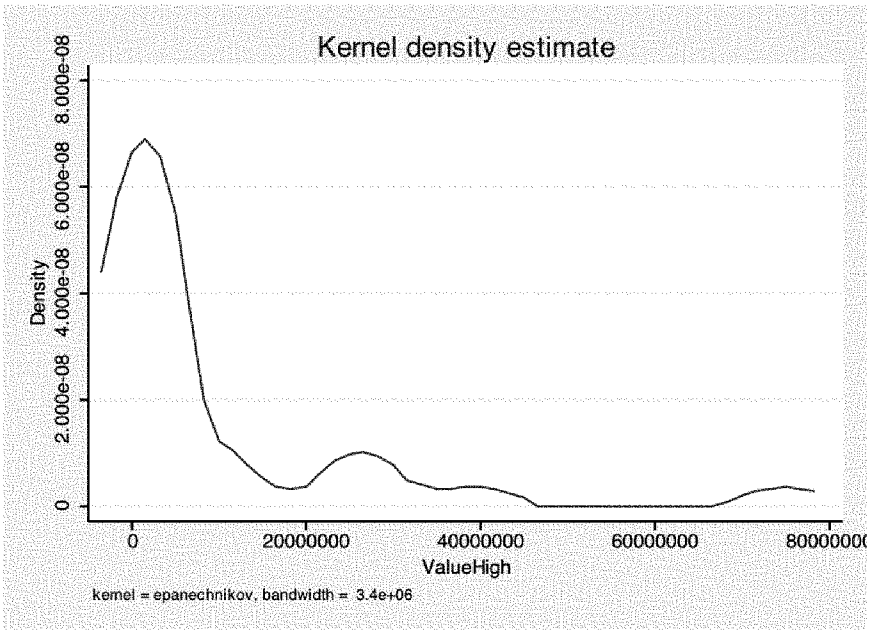

Figure 4. Confidence Intervals, Lognormally Distributed High Estimates

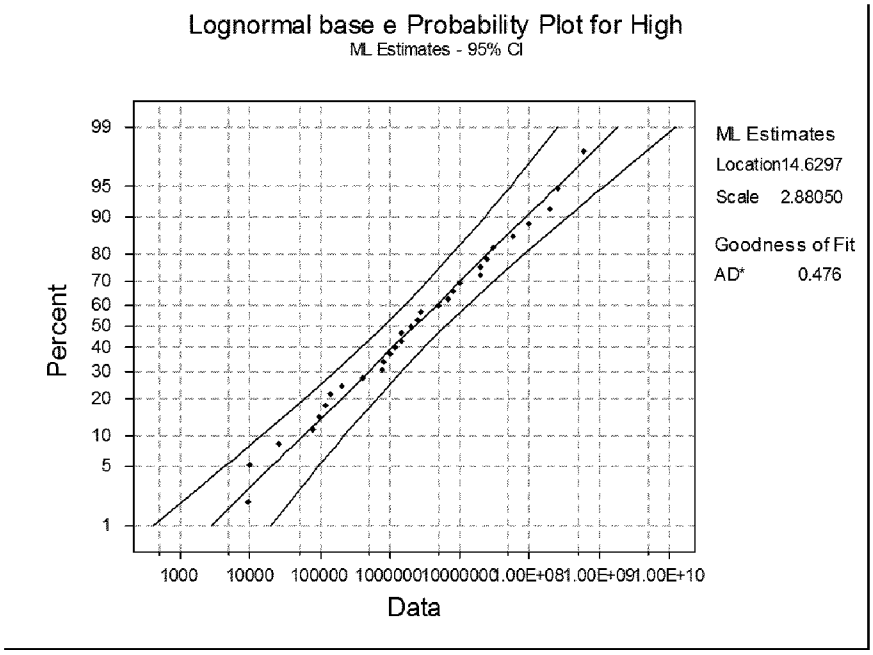

Table 2: Paired T-Test for Difference between Low and High Estimates

Paired Sample Statistics					
	Mean	N	Std. Dev.		
ln (Low)	12.33	16	2.04		
ln (High)	14.91	16	2.73		
Paired Sample Correlations					
	N	Correlation	Sig.		
ln (Low) & ln (High)	16	0.46	0.07		
Paired Samples Test					
Paired Differences					
ln (Low) –ln (High)		95% Confidence Interval of the Difference			
Mean	Std. Dev.	Lower	Upper	df	Sig. (2-tailed)
-2.58	2.54	-3.93	-1.22	15	0.001

Figure 5: Probability Plot, High and Low Estimates

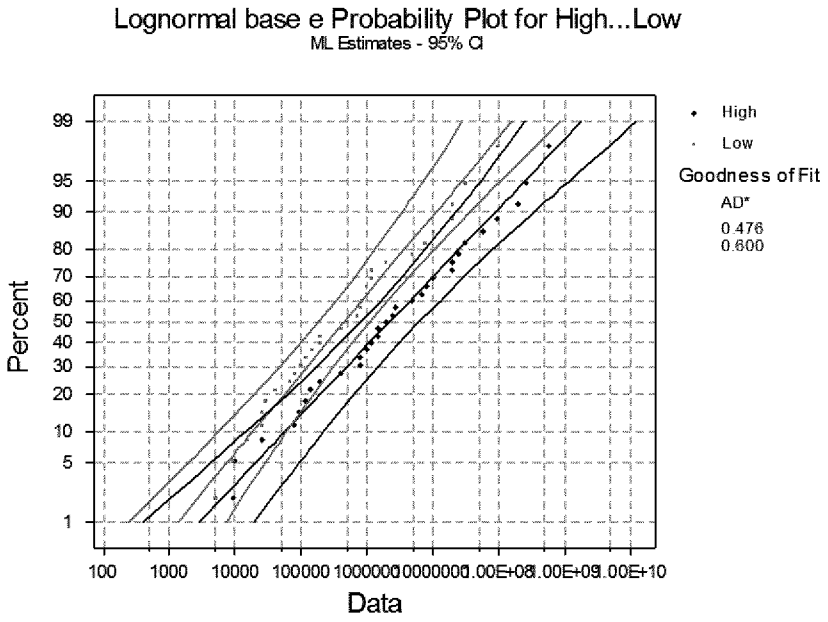

Table 3: Incarceration and Corresponding Offence Points

	Range of Months of Incarceration	
Offence Points	**Incarceration Minimum**	**Incarceration Maximum**
8	0	6
9	4	10
…	…	…
14	15	21
15	18	24
16	21	27
…	…	…
42	360	Life

Table 4: Calculation of Base Offence Level

Base Offence Points	**Adjustment**
6	Base Offence level according to DOJ Manual
+2	Assumed for all defendants (for more than minimal planning (according to Zwillinger et al))
–2	Assumed for all defendants (for acceptance of responsibility (according to Zwillinger et al))
6	Subtotal
+2	If Charged with 1831 (economic espionage, which has a higher offence level)
+2	If considered "insider" (also a higher offence level)
	Total, then cross-referenced with Sentencing Guidelines

Table 5: Offence Points Based on Value of Stolen Trade Secret

Points	**Value of Stolen Trade Secrets**
0	$ 5,000
2	$ 5,000
4	$ 10,000
6	$ 30,000
8	$ 70,000
…	…
30	$ 400,000,000

Figure 6. Distribution of X_{ref} Values

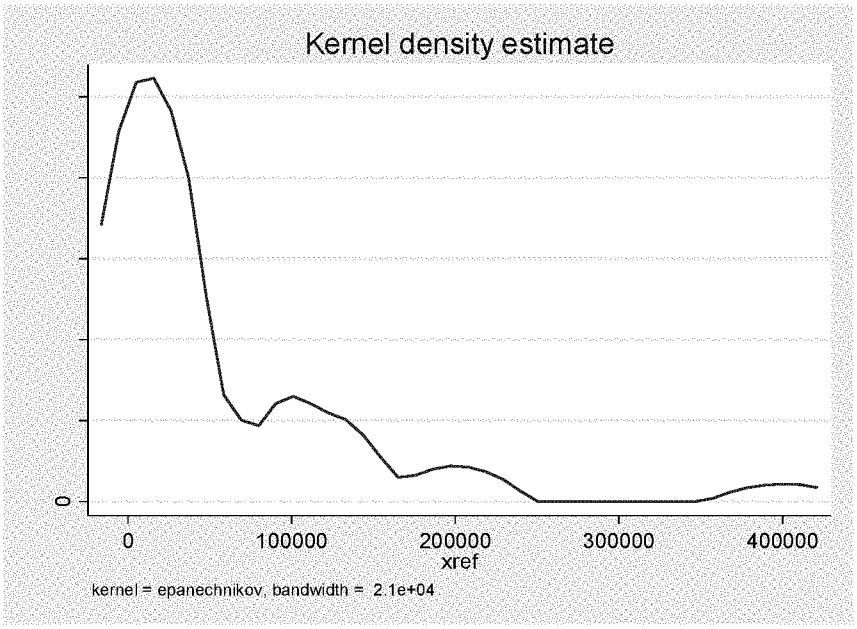

Table 6: Wilcoxon Signed-Rank Comparison, Cross-Reference and High[145]

Ranks					
			n	Mean Rank	Sum of Ranks
X_{ref} – High	Negative Ranks	X_{ref} < High	19	10.37	197
	Positive Ranks	X_{ref} > High	1	13	13
	Ties	X_{ref} = High	0		
	Total		20		
Test Statistics					
	Z	Asymp. Sig. (2-tailed)			
X_{ref} – High	-3.435	0.001			

[145] For this table and the next, the asymptotic significance for the Z-stat is two tailed.

Table 7: Wilcoxon Signed-Rank Comparison, Cross-Reference and Low

Ranks					
			n	Mean Rank	Sum of Ranks
X_{ref} − Low	Negative Ranks	X_{ref} < Low	16	11.25	180
	Positive Ranks	X_{ref} > Low	4	7.50	30
	Ties	X_{ref} = Low	0		
	Total		20		
Test Statistics					
	Z	Asymp. Sig. (2-tailed)			
X_{ref} − Low	-2.800	0.005			